In less than a generation, our society has so embraced the interconnectivity of the Internet that we are not only totally dependent upon it to drive the engines of our economy and provide the essential services of our government, but we are also more vulnerable than ever to attack and disruption.

As America's infrastructure and commerce are increasingly wired to the web, we have allowed gaping holes for hackers, including hostile foreign governments and terrorists, to exploit. If business and government have been slow to adequately defend against damaging and costly cyber espionage and cyber-attack, they have also been unable to share information and resources in order to more effectively combat them.

Business and government are on the front lines of the world's most sophisticated hacking attacks. Unfortunately, experts tell us that private data networks are especially vulnerable and many businesses don't even know their sensitive data and records have been plundered and stolen.

The FBI's top cyber security authority recently admitted that America is losing ground in its ability to stay ahead of computer hackers. Even worse, U.S. businesses are being compromised without anyone noticing.

"We have found their data in the middle of other investigations," FBI executive assistant director Sean Henry recently told the Wall Street Journal. "They are shocked and, in many cases, they've been breached for many months, in some cases years, which means that an adversary had full visibility into everything occurring on that network, potentially."

Such attacks, if limited, might not raise alarms, but the FBI and other watchdogs tell us foreign governments and international criminals, including terrorists, are actively probing and getting access to information that could compromise both our economy and our national security. In our society, where business and government work hand in hand, theft of sensitive information stored on corporate networks can cause as much harm as the penetration of our government's own data systems.

Current law prevents the government from sharing information about attacks on American businesses with those same companies. This gap in our security is being exploited by professional hackers backed by foreign governments, including China and Russia. These attacks come at a high cost to our economy as vital American business data is stolen and used against us. China, in particular, has been aggressively seeking to gain information from American corporate and government computer networks.

American companies are in the crosshairs of Chinese hackers probing for information about mergers and acquisitions, pricing, and research and development efforts. Such industrial espionage ultimately targets American jobs. Each year, critical data equivalent to the entire print collection of the Library of Congress is stolen from American industry and individuals.

How can we stop these cyber-attacks? According to the experts, the only way to get ahead of these advanced, persistent cyber threats is to take them just as seriously as physical threats to our country. That means government and business should not only devote resources to counter aggressive cyber threats, but they must also work together as much as possible to plug the holes in our defenses.

Last week, the House passed the Cyber Intelligence Sharing and Protection Act to begin the process of closing the gaps in America's data security fence. The legislation will allow the U.S. government to share classified cyber threat intelligence with the private sector to help them better defend their networks. Furthermore, the legislation encourages, but does not mandate, business to share similar information about security threats with the government.

Keeping in mind the obligation to safeguard Americans' right to personal privacy, the legislation only allows the sharing of information related to advanced cyber espionage and cyber-attack. It also encourages the private sector to "anonymize" or "minimize" information it voluntarily shares with others, including the government. Government use of shared data would be limited and any misuse of that data would be subject to federal lawsuit.

Hostile foreign governments and terrorists intent on harming our country are outsmarting America's on-line defenses as they seek to steal business and government secrets and degrade our economic and military advantages. Failure to take this threat seriously will only jeopardize American jobs and potentially put American lives at risk.

The passage of the Cyber Intelligence Sharing and Protection Act is bad news for Chinese and Russian hackers who will have to work even harder to break through our cyber defense.

My staff and I work for you. If we can ever be of service, do not hesitate to call my office toll free at 1-800-288-8721.

For release: April 30, 2012